SECNAV/OPNAV
BEST PRIVACY PRACTICES

Please direct any questions/concerns to

Doris Lama 202-685-6545

GOAL

- Think Privacy when conducting business.
- Ensure that all members of our staff employ best business practices when collecting, maintaining, disseminating or disposing of personally identifiable information (i.e., Information about an individual that identifies, relates to, is unique to, or describes that person, such as home address, date of birth, SSN, home phone, credit card number, etc).
- Eliminate the potential for Identity Theft.

BEST PRACTICES

- Think Privacy when collecting information. If you need to solicit personal information directly from an individual, ensure you have a Privacy Act Statement that provides the following information:
  - **Authority that authorizes collection of information, such as 20 U.S.C. 5013, Secretary of the Navy**
  - **Purpose: Why are you collecting the information?**
  - **Routine Uses: Who will routinely have access to the information?**
  - **Disclosure: Voluntary. However, failure to provide the requested information may result in _____.**
  - **NOTE: Avoid collecting the entire SSN whenever possible. Consider just collecting the last four digits instead.**

MORE BEST PRACTICES

- PROPERLY MARK DOCUMENTS AT TIME OF ORIGINATION
  - This alerts the recipient as to how to handle a document that contains personal information. For example, when transmitting name and SSN, mark the document FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure may result in both civil and criminal penalties.
  - For messages containing personal information, such as SSN, date of birth, etc., simply mark the document “(FOUO)” in the subject block.

MORE BEST PRACTICES

- PROPERLY DISPOSE OF DOCUMENTS CONTAINING PERSONAL INFORMATION TO AVOID IDENTITY THEFT
  - Shred or burn all documents that contain personal information
  - DO NOT ASSUME that information being placed in a recycle bin is being shredded prior to sale or disposal.

MORE BEST PRACTICES

- **Ensure access to documents containing personal information is limited to those individuals with an official need to know - not a want to know.**
- **Do not place documents in areas where they can be viewed by individuals that do not have an official need to know.**
- **Control the dissemination of documents containing personal information so that they are not compromised.**
- **If you are maintaining a data base that contains personal information, ensure that there is an approved Privacy Act systems of records notice to cover the collection. Contact CNO (DNS-36) for assistance.**
- **Do not place documents containing personal information in public folders on your computer.**
- **Do not place the name and SSN in the subject line of an email or letter.**
- **Do not place documents in file folders that are retrieved by an individual's name and/or personal identifier unless there is a Privacy Act system of records notice that allows the collection of information.**

MORE BEST PRACTICES

- **When you receive an email and it contains personal information about another individual, do not forward that document to others without first assessing whether each recipient has a need to know.**

- **Use training to educate your personnel on Privacy.**

  - **Ensure all newly assigned personnel receive orientation training on the Privacy Act so they fully understand their role in ensuring that personal information is protected from unauthorized disclosure.**

  - **Ensure all personnel receive refresher training once a year or more often should they be involved in a breach (loss) of personal information.**

  - **Ensure that supervisors take Privacy Act training 102 from http://privacy.navy.mil**

  - **Ensure all personnel who deal with personal information contained in a Privacy Act system of records are properly trained on the systems notice and the safeguards addressed therein and the restrictions regarding access to the information.**

REVIEW BUSINESS PRACTICES

- Review how information is stored and transmitted, as a breach, loss or compromise of information is costly to the government, to the individual whose identity is at risk, and to the individual who is involved in the loss/ compromise/theft.

- Individuals who use laptops, blackberrys, etc., must comply with DON directives/guidance on how to prevent loss.

LOSS OF PRIVACY INFORMATION

- If you lose personal information, you must report that loss immediately to the head of your organization, as there are distinct reporting requirements that must be followed.
- When in doubt, contact DNS-36 at 202-685-6545.

EXAMPLES OF REPORTED LOSSES

- Laptop computer containing personal information was left in car that was vandalized
- Documents containing names and SSNs were disposed of in dumpster and papers found blowing in wind
- Computer database accessed by unauthorized persons
- Memory stick lost to computer
- Personal information placed in public folder on website
- Messages containing SSNs not properly marked

DON CODE OF PRIVACY ACT FAIR INFORMATION PRINCIPLES

- **DON has devised a list of principles to be applied when handling personal information. This is referred to as the DON Code of Privacy Act Fair Information Practices.**

- **Any DON employee, military member, or contractor who handles the personal information of others must abide by the principles set forth by the Code.**

The DON Code of Fair Information Principles

1. <u>The Principle of Openness</u>: When we collect personal data from y we will inform you of the intended uses of the data, the disclosures t will be made, the authorities for the collection, and whether the coll is mandatory or voluntary. We will collect no data subject to the Priv unless a Privacy Act system notice has been published in the Federal Register and posted on the and at http://privacy.navy.mil .

2. <u>The Principle of Individual Participation</u>: Unless DON has claimed exemption from the Privacy Act, we will, upon request, grant you acc your records; provide you a list of disclosures made outside the Depa of Defense; and make corrections to your file, once shown to be in er

3. <u>The Principle of Limited Collection</u>: DON will collect only those pe data elements required to fulfill an official function or mission groun law. Those collections are conducted by lawful and fair means.

The DON Code of Fair Information Principles (cont'd)

4. The Principle of Limited Retention: DON will retain your personal information only as long as necessary to fulfill the purposes for which is collected. Records will be destroyed in accordance with establishe records management principles.

5. The Principle of Data Quality: DON strives to maintain only accu relevant, timely, and complete data about you.

6. The Principle of Limited Internal Use: DON will use your personal only for lawful purposes. Access to your data will be limited to those Department of Defense individuals with an official need for access.

7. The Principle of Disclosure: DON employees and military member zealously guard your personal data to ensure that all disclosures are with your written permission or are made in strict accordance with t Privacy Act.

The DON Code of Fair Information Principles (cont'd)

8. **<u>The Principle of Security</u>: Your personal data is protected by appr safeguards to ensure security and confidentiality. Electronic syste be periodically reviewed for compliance with the security principle Privacy Act, the Computer Security Act, and related statutes. Elec collections will be accomplished in a safe and secure manner.**

9. **<u>The Principle of Accountability</u>: DON and our employees, military members, and contractors are subject to civil and criminal penalti certain breaches of Privacy. DON is diligent in sanctioning individ who violate Privacy rules.**

10. **<u>The Principle of Challenging Compliance</u>: You may challenge DON you believe that DON has failed to comply with these principles, t Privacy Act, or the rules of a system of records notice. Challenges addressed to the person accountable for compliance with this Cod local Navy/Marine Corps Privacy Act manager, CNO (DNS-36), or CMC (ARSF).**